



1/8  
H.ETOH,ET AL  
JP919990295

## STACK PROTECTION SYSTEM

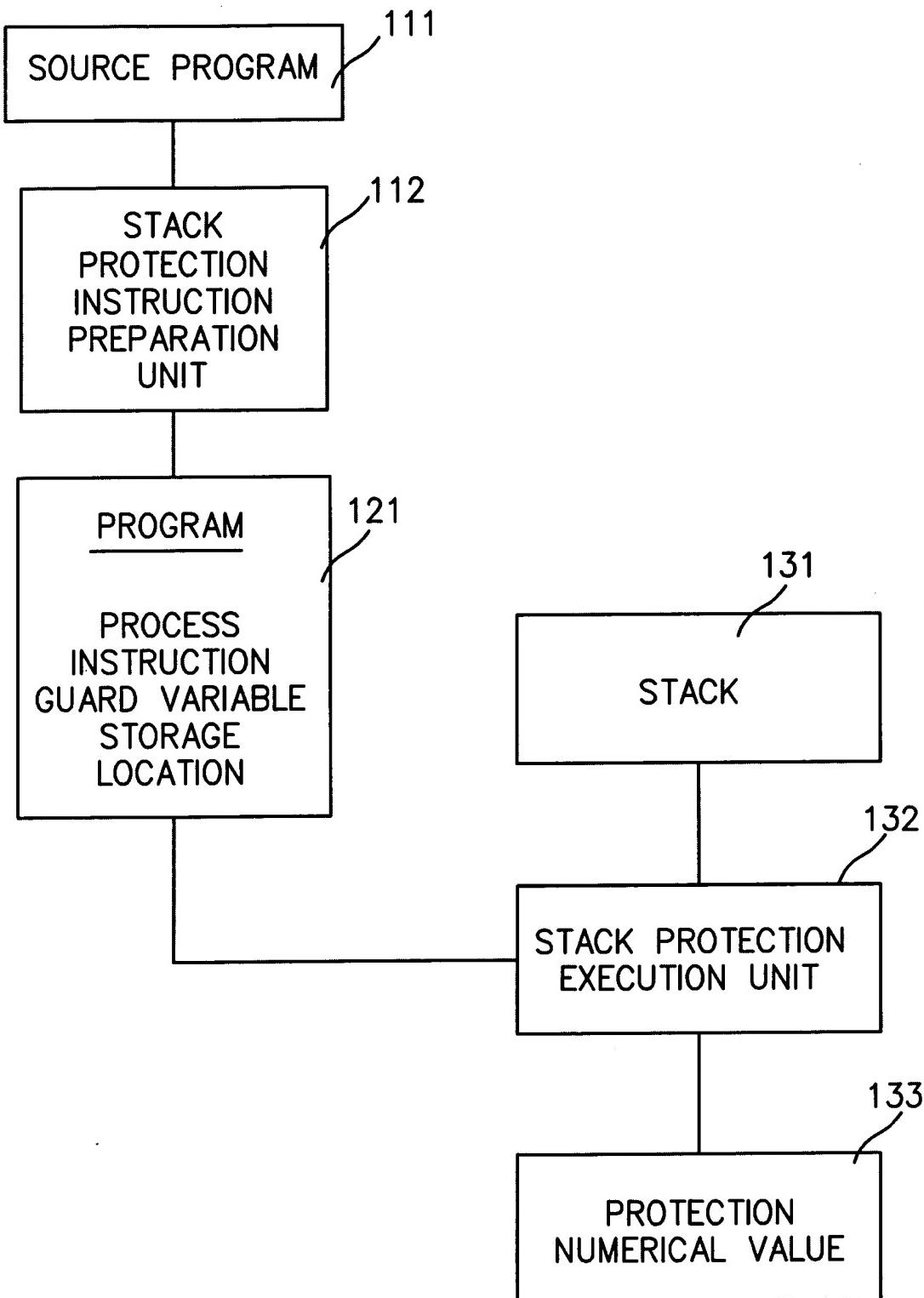


FIG.1



2/8  
JP19990295

## MEMORY PATTERN WHEN GUARD VARIABLE IS STORED

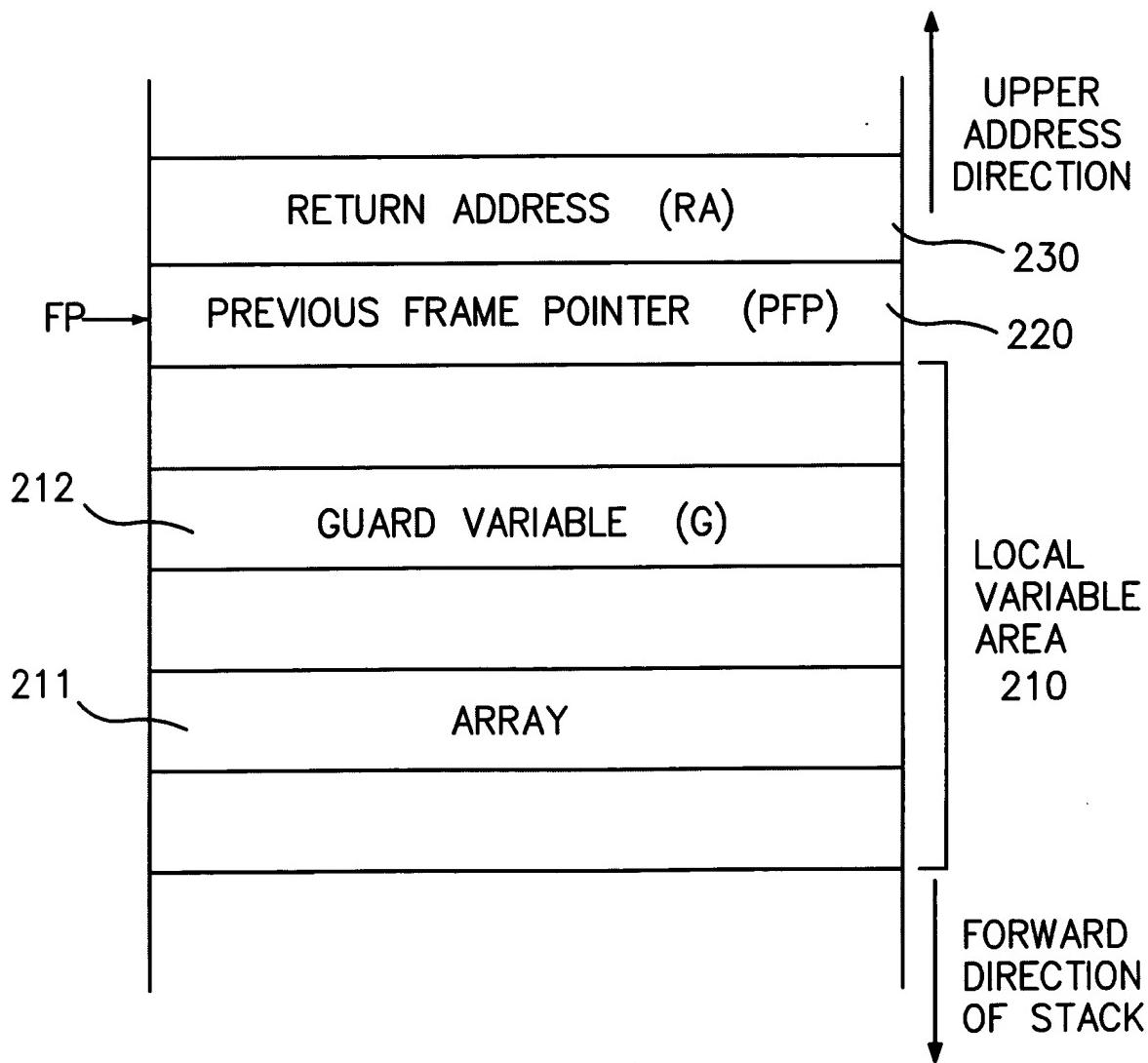


FIG.2



3/8  
JP919990295

## PROCESSING OF STACK PROTECTION INSTRUCTION PREPARATION UNIT 112

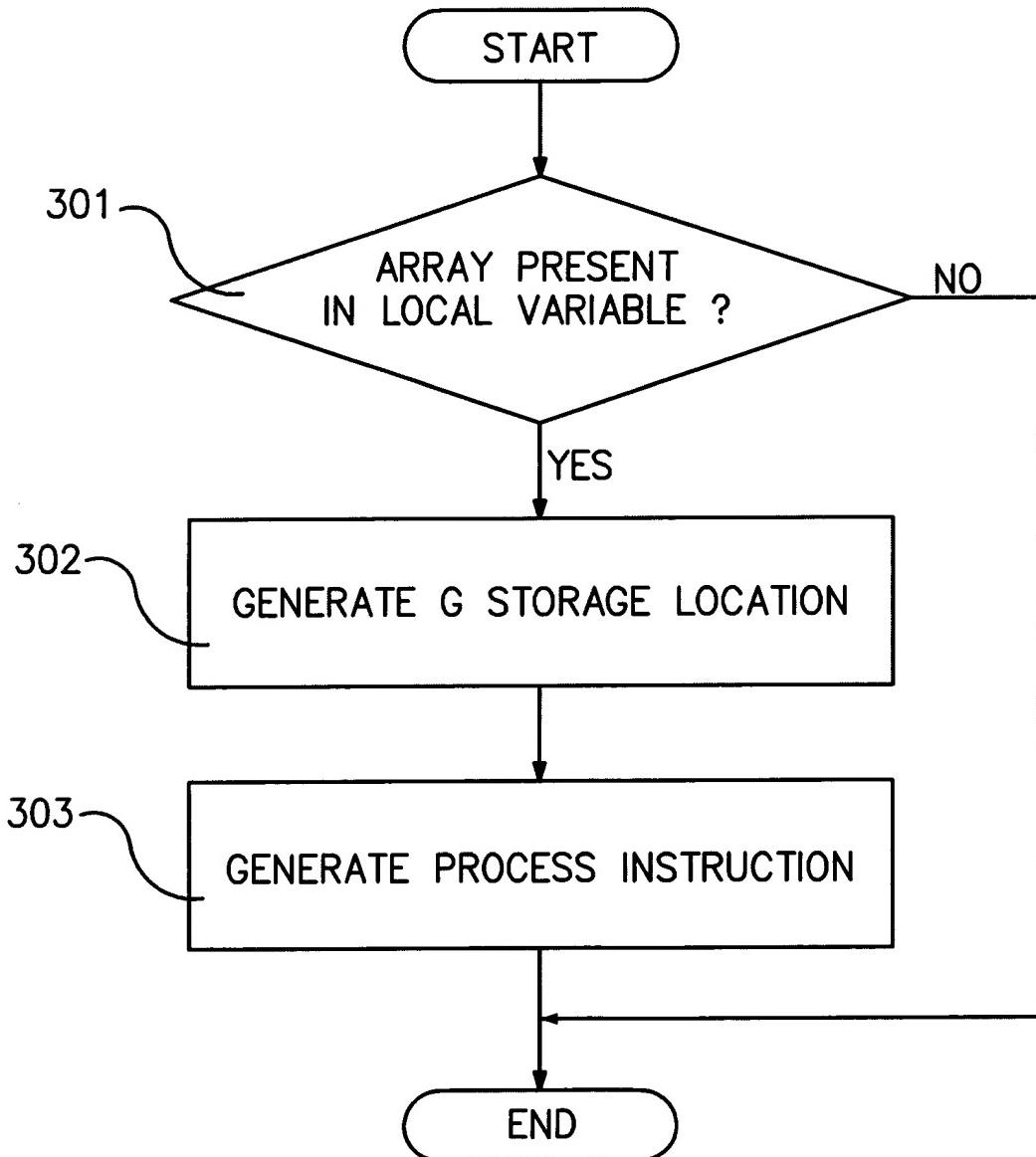


FIG.3

## PROCESSING OF STACK PROTECTION EXECUTION UNIT 132

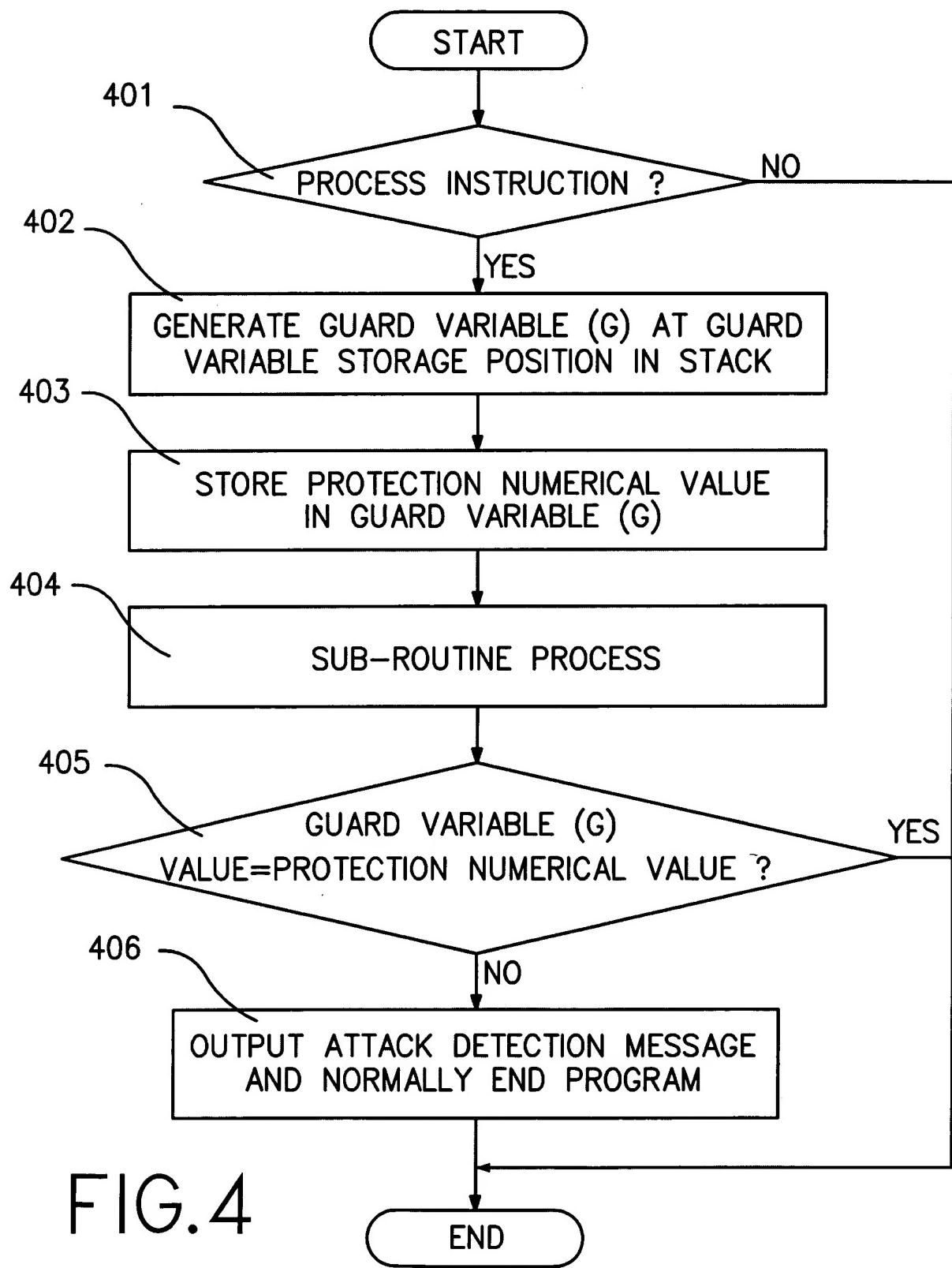


FIG.4



5/8  
JA919990295

- variable declaration  
volatile int guard;
- function entrance  
gv=guard\_value;
- function exit  
if(gv!=guard\_value){  
/\*output error log\*/  
/\*halt execution \*/  
}

FIG. 5

```
void foo()  
{    volatile int guard; ← 601  
    char buf[128];  
  
    gv=guard_value; ← 602  
    ---  
    stropy (buf,getenv ("HOME"));  
    ---  
    if(gv!=guard_value){  
        /*output error log*/ ← 603  
        /*halt execution */  
    } }
```

FIG. 6



6/8  
JP919990295

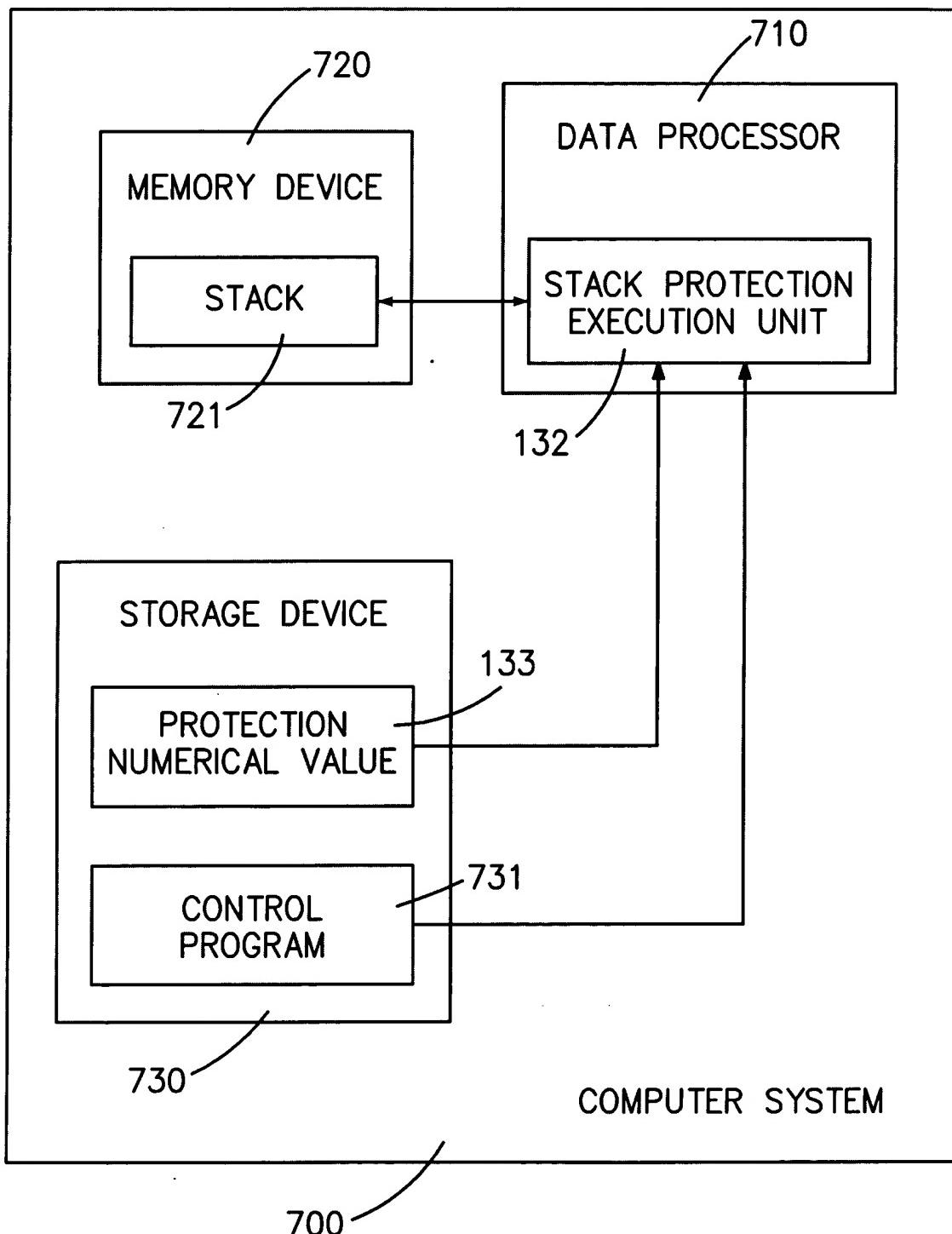
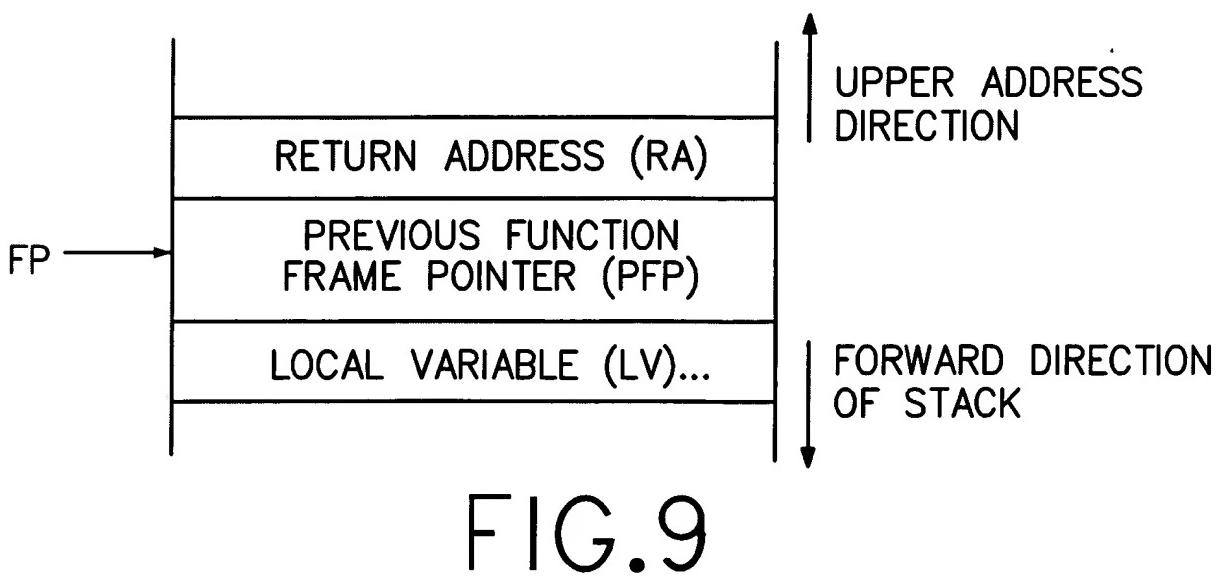
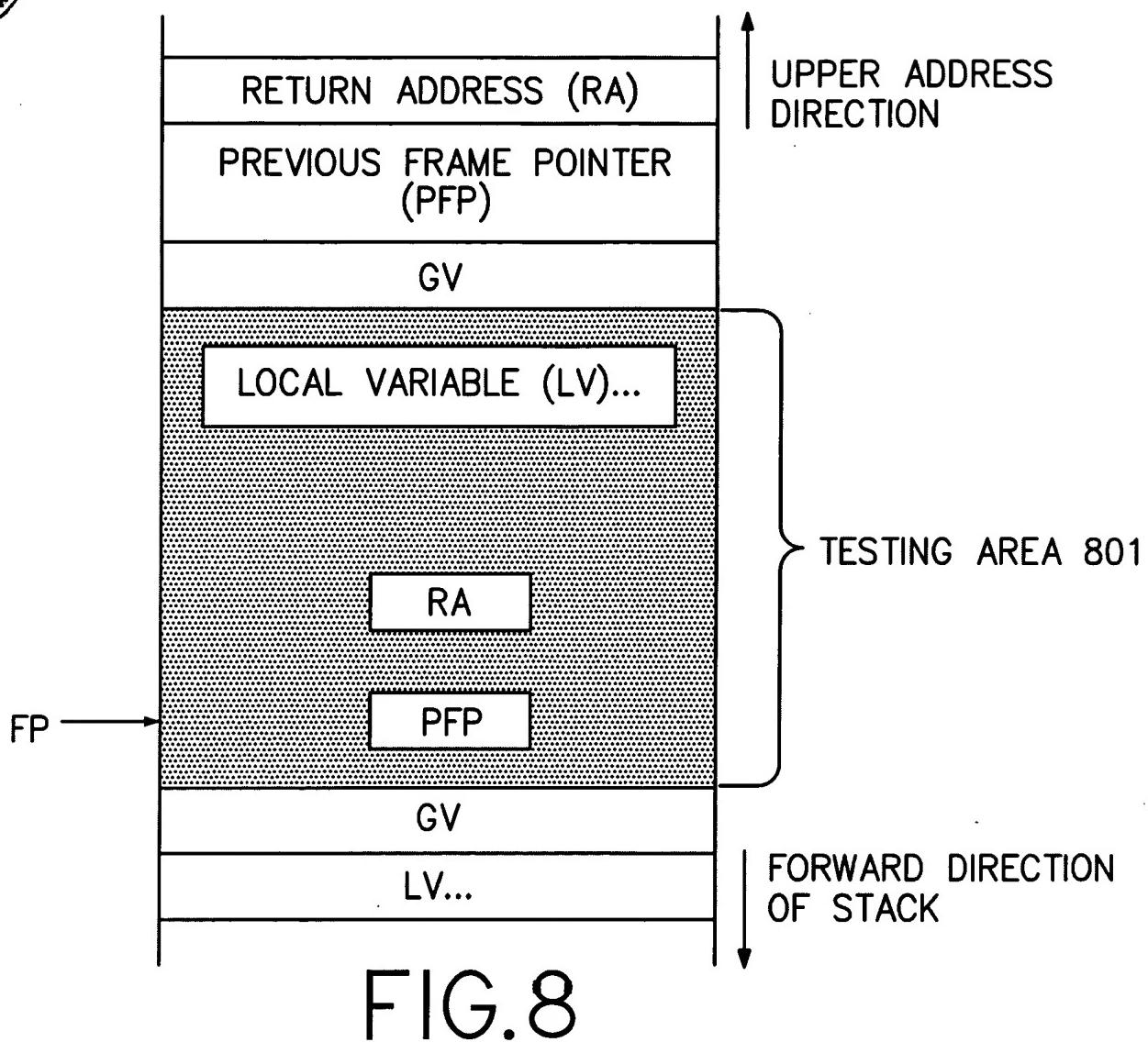


FIG. 7



7/8  
JA919990295





8/8  
JA19990295

```
void foo()
{
    char buf[128];
    — — —
    strcpy (buf,getenv ("HOME"));
    — — —
}
```

FIG.10

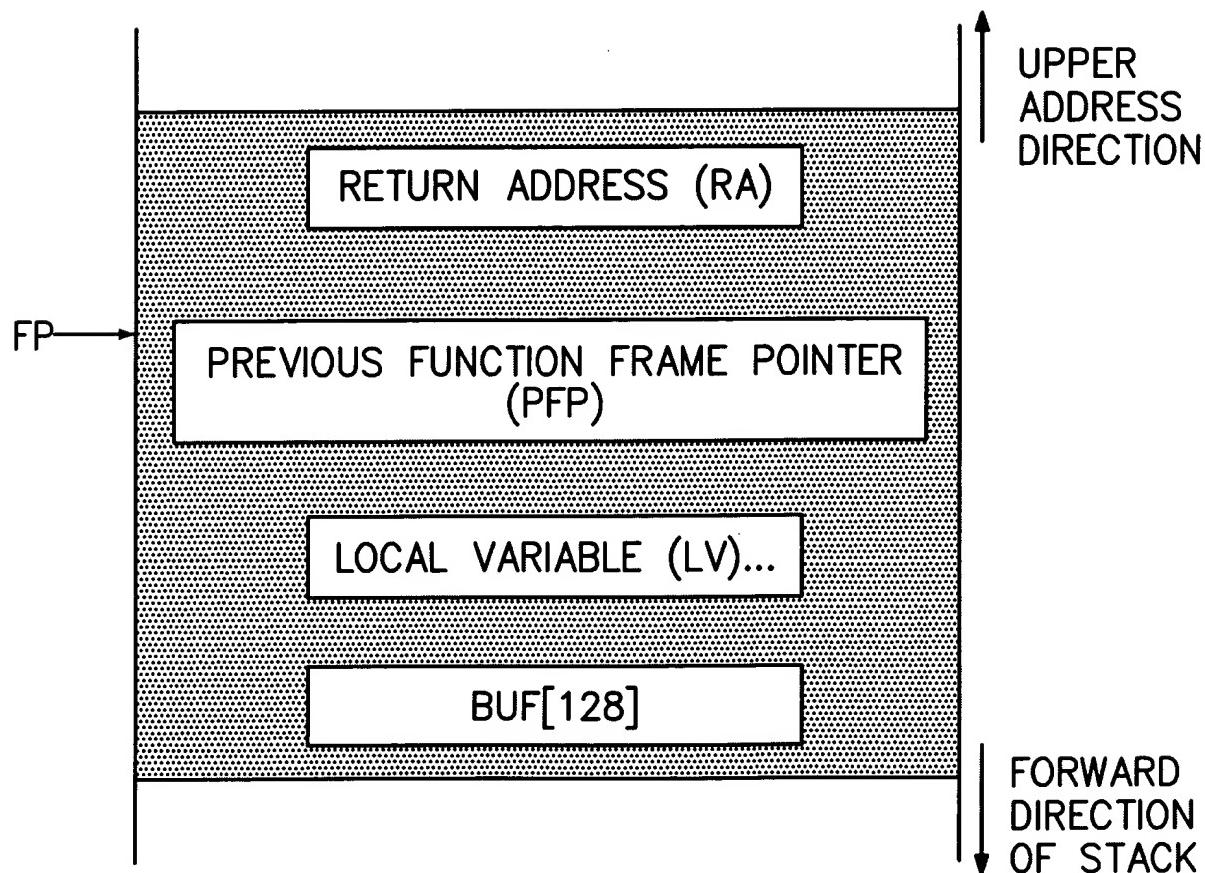


FIG.11